Judge Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	NO. CR15-5351RJB UNITED STATES' SURREPLY TO DEFENDANT'S MOTION TO SUPPRESS **(Filed Under Seal)**

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, Matthew P. Hampton and Andre Penalver, Assistant United States Attorneys for said District, and Keith A. Becker, Trial Attorney, hereby files this surreply to the Defendant's Motion to Suppress Evidence and Statements.

In the reply brief, the defense raises new arguments and misstates important points of law and fact relevant to the Court's analysis. Among other things, the defense applies the wrong test regarding the intent of law enforcement; the defendant misreads the DOJ Electronic Evidence Manual and the amendments to Rule 41; finally, the defendant misstates the nature of a computer's IP address. The government addresses each of these problems in turn.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

I. Law enforcement did not violate Rule 41, intentionally or otherwise.

The search warrant at issue was authorized by a United States Magistrate Judge in the Eastern District of Virginia permitting the government to employ a NIT to unmask the IP address of users of the designated web-based bulletin board. The warrant was obtained in the district where (1) the server was located, (2) the communications among users occurred, (3) the NIT authorized by the warrant was to be deployed, and (4) the information obtained through the use of the NIT was collected. As discussed in the government's response, the authorization of the NIT warrant did not violate Rule 41.

In any event, even if this Court finds that the court-authorized use of a NIT violated Rule 41, suppression is neither required nor reasonable in this case. Where law enforcement sought and obtained a warrant upon finding of probable cause, to warrant the extreme remedy of suppression, the violation must be "fundamental," that is of constitutional magnitude, something that is not the case here. A mere technical error may result in suppression only where a defendant can establish prejudice or that law enforcement intentionally and deliberately disregarded Rule 41. *See United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992). Here, although the defense suggests otherwise, even if a defendant wants to seek to hide his Internet Protocol address through the use of Tor, that does not cloak the IP address with an expectation of privacy. That IP address is essential to be able to route communications in the same way that a telephone number routes a telephone call. Therefore, whether routed first through a "node" or done directly, IP addresses simply are not private.

Although Michaud argues to the contrary (Dkt. 69, p. 20), the Ninth Circuit has consistently equated "intentional and deliberate disregard" with "bad faith." In *United States v. Williamson*, 439 F.3d 1125, 1134 (9th Cir. 2006)—a case that Michaud cites—the Ninth Circuit affirmed the trial court's denial of a motion to suppress for a Rule 41 violation where the agent acted intentionally but nonetheless was found to have acted "acted in good faith." *Id*. There are numerous similar examples where the Ninth

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Circuit announces that premise.[1] Michaud cites no case suppressing evidence for the type of Rule 41 violation alleged in this case. Indeed, a diligent search has identified no such case. On the other hand, as noted in the government's response, similar warrants have been issued in other cases and the resulting evidence has not been suppressed. *See, e.g., United States v. Pierce et. al.*, D. Neb., No. 13-cr-106; *United States v. John Doe #1 et. al.*, D. Neb., No. 13-cr-107; *United States v. Cottom et. al.*, D. Neb., No. 13-cr-108. Indeed, in the case that Michaud himself has cited, the district court did not suppress evidence in a case involving similar circumstances. *See United States v. Cottom, et. al.*, D. Neb., No. 13-cr-108.

Michaud's reliance on *United States v. Gantt*, 194 F.3d 987, 994-95 (9th Cir. 1999) (overruled on other grounds, *United States v. W.R. Grace*, 526 F.3d 499, 506 (9th Cir. 2008)) is also misplaced. In *Gantt*, the Ninth Circuit granted the motion to suppress based on a showing that officers had deliberately violated Rule 41(d) by failing to provide the defendant with a copy of the warrant. In contrast, in this case, the agents sought and obtained authorization from a judge to do the very actions that the defense is now complaining about here. They did not act with an intention to violate the law but rather sought authorization from a court to comply with the law under unusual circumstances and for the purpose of obtaining information that at bottom is not something in which a defendant has an expectation of privacy. As the government noted in its initial response, when Michaud communicated with Website A, he voluntarily reached into the Eastern District of Virginia in order to download the content of the website, which included the court-authorized NIT instructions. While the location of his computer was then unknown, the NIT was only deployed to Michaud's computer as a

---

[1] *See, e.g., United States v. Crawford*, 657 F.2d 1041, 1048 (9th Cir. 1981) (affirming denial of motion to suppress for purported Rule 41 violation without evidence of "bad faith"); *United States v. Ritter*, 752 F.2d 435, 441 (9th Cir. 1985)("This court requires more than a violation [of Rule 41 to warrant suppression of evidence]; there must be either a fundamental violation of the Rule or a bad faith violation of the Rule."); *United States v. Luk*, 859 F.2d 667, 673-74 (9th Cir. 1988))(affirming denial of motion to suppress for Rule 41 violation where court found no "deliberate disregard or bad faith" on the part of agents); *United States v. Martinez-Garcia*, 397 F.3d 1205, 1214 (9th Cir. 2005) (finding officers serving a warrant "did not act in intentional or deliberate disregard of Rule 41" where the "officers had good faith reasons" to withhold service of a warrant).

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

result of his voluntary action to communicate with a computer in EDVA, where he obtained the NIT instructions (and accessed child pornography). Under normal use of the Internet, that communication to the site would have revealed Michaud's IP address to the web server. The authorized NIT merely caused Michaud's computer to send such information into the District.

In support of his claims, Michaud points to an amendment to Rule 41 that the government had proposed, and a dated government-issued manual to argue that the affiant for the NIT warrant should have known that the NIT search proposed would violate Rule 41. But these claims fall wide of the mark.

The proposed amendment to Rule 41 was designed to clarify that courts have venue to issue a warrant "to use remote access to search electronic storage media" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means." This proposed amendment and the accompanying letter from the then Assistant Attorney General for the Criminal Division of the Department of Justice do not support the conclusion that the actions in this case violate Rule 41. That the Department of Justice seeks greater clarity in the rule does not convert conduct taken in good faith to a deliberate and intentional violation of the rule. Moreover, at the time the Department of Justice proposed the Rule 41 Amendment, a single magistrate judge in one case had rejected a warrant to locate a computer concealed through technological means, but every other magistrate judge known to consider the issue had issued such a warrant.[2]

Portions of the letter that Michaud does not cite make this clear. For example, the letter recognizes that under Rule 41, "even when investigators can satisfy the Fourth Amendment's threshold for obtaining a warrant for the remote search—by describing the

[2] Nor is such a clarification unusual. For example, Rule 41 was amended in 2002 to add "information" to the definition of "property" in Rule 41(a)(2)(A), even though the Supreme Court had previously held in *United States v. New York Tel. Co.*, 434 U.S 159, 169 (1977) that the then-existing definition of "property" (which included "documents, books, papers and any other tangible objects") was broad enough to include intangible information. *See* Amendments to the Federal Rules of Criminal Procedure, 207 F.R.D. 89, 283 (2002).

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

computer to be searched with particularity and demonstrating probable cause to believe that the evidence sought via the remote search will aid in a particular apprehension or conviction for a particular offense—a magistrate judge *may* decline to issue the requested warrant." *Id*. at 2 (emphasis added). The letter then notes that "the Fourth Amendment permits warrants to issue for remote access to electronic storage media or electronically stored information," while acknowledging that "Rule 41's language does not anticipate those types of warrants in all cases." *Id*. at 3. And most importantly, the letter specifies that "[a]mendment is necessary to *clarify the procedural rules* that the government should follow when it wishes to apply for these types of warrant." *Id*. at 3 (emphasis added). The government has never suggested that Rule 41 did not already permit such searches.

Michaud also cites objections to the proposed amendment by various organizations and uses this objection to assert that the proposed amendment consists of efforts by the government to "vastly expand its search and surveillance powers," which have "not been successful" (Dkt. 69, pp. 4, 6). To the contrary, the amendment has been approved by the Advisory Committee on Criminal Rules, the Standing Committee, and the Judicial Conference of the United States; it is currently under review by the Supreme Court. *See* Transmittal of Proposed Amendments to the Federal Rules at 8 (available at http://www.uscourts.gov/rules-policies/pending-rules-amendments). As Judge Jeffrey Sutton explains in the Summary of Proposed Amendments to the Federal Rules, "[m]uch of the opposition [to the proposed amendment] reflected a misunderstanding of the scope of the proposal. The proposal addresses venue; it does not itself create authority for electronic searches or alter applicable statutory or constitutional requirements." *Id*.

Michaud similarly claims that information contained in a 2009 manual published by the Department of Justice indicates that the government violated Rule 41 and that such a violation was deliberate. That is also not the case. This manual is now six years old. It was prepared to provide assistance to prosecutors and to reflect the thinking a particular point in time, and not the official position of the Department of Justice on any point in

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

law. More importantly, this manual has no regulatory effect, confers no rights or remedies, and does not have the force of law or a U.S. Department of Justice directive. *See United States v. Caceres*, 440 U.S. 741 (1979).

In any event, as with the letter and proposed amendment, the manual does not state that it is or would be a violation of Rule 41 or the Fourth Amendment for a court to issue a warrant authorizing use of a NIT in the particular circumstances of this case, nor does it contain a legal analysis of how Rule 41 applies to the particular circumstances of this case.[3] The mere recognition, expressed in the proposed amendment or Department of Justice manual, of the possibility that a particular judge may interpret Rule 41 so as to deny a requested warrant, is light-years away from a concession that such an interpretation is correct, let alone evidence to indicate that by requesting and obtaining court-authority to conduct a search from a judge who did not interpret Rule 41 to prohibit such a request, law enforcement acted in intentional and deliberate disregard of the rule. The defendant's complaint lies with the issuing magistrate, not with law enforcement.

II. Tor use does not confer a reasonable expectation of privacy in IP address information when its users voluntarily give up such information to third parties.

In its initial response, the government argued that Michaud lacks a reasonable expectation of privacy in IP address information collected via the NIT–which is pertinent to the Court's analysis of the Fourth Amendment issues underlying the NIT authorization and its reasonableness. Dkt. 47, pp. 16, 19. Michaud contends that his use of Tor confers an expectation of privacy upon IP address information. That is not correct and is premised upon a misunderstanding of how Tor works. While Michaud may have a reasonable expectation of privacy in stored information contained on his computer, he

[3] In fact, the section of the manual Michaud cites specifically notes that in the event "agents do not and even cannot know that data searched from one district is actually located outside the district, evidence seized remotely from another district ordinarily should not lead to suppression of the evidence obtained." "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" at 85 available at: http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

lacks a reasonable expectation of privacy in IP address information that belongs to an internet service provider and that is voluntarily shared with others in the course of Internet communications. Dkt. 47, p. 19. His use of Tor does not alter that.

As publicly available information on the Tor Project website demonstrates, Tor's fundamental design requires users to disclose information, including their IP addresses, to unknown volunteers running Tor "nodes," so that their communications can be directed toward their destinations. Ex. 1, "Tor Project: Overview."[4] Tor users thus voluntarily entrust their communications not only to a third party such as an internet service provider, but to an unknowable collection of strangers. Accordingly, when Michaud states that "a computer user who accesses a web site through the Tor network does not need to convey his or her IP address" (Dkt. 69, p. 15), that is incorrect. Tor routes communications through multiple computers in order to mask the origin of the communication–"similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you"–but user IP addresses are still relayed to nodes on the Tor network. Ex. 1 at 2.[5]

[4] Available at: https://www.torproject.org/about/overview.html.en (last visited Dec. 9, 2015).

[5] Moreover, Tor users share their communications with these unknown and unknowable volunteers despite public acknowledgment by the Tor Project that the Tor network has vulnerabilities. The Tor Project overview notes that "Tor can't solve all anonymity problems" and that a user needs to "use protocol-specific support software if you don't want the sites you visit to see your identifying information." *Id*. The Tor Project also publishes a "Frequently Asked Questions" or "FAQ" page, in which it posts the question: "[s]o I'm totally anonymous if I use Tor?" and the response, "[n]o." Ex. 2, "Frequently Asked Questions," p. 23.[5] That same section of the FAQ specifically warns users that certain computer applications may "bypass Tor and share information directly to other sites on the Internet." *Id*. Tor users, like all Internet users, thus lack a reasonable expectation of privacy in IP address information shared while using the Tor network.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

III. CONCLUSION

For all the foregoing reasons, the Court should deny Defendant's motion to suppress.

DATED this 21st day of December, 2015.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

/s/ Matthew P. Hampton
Matthew P. Hampton
Andre M. Penalver
Assistant United States Attorney
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
Telephone: (253) 428-3800
Fax: (253) 428-3826
E-mail: matthew.hampton@usdoj.gov
andre.penalver@usdoj.gov

STEVEN J. GROCKI
Chief

/s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on December 21, 2015, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney of record for the defendant.

/s/ Matthew Hampton
Matthew P. Hampton
Assistant United States Attorney

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800